Office of Legislative Research
Research Report

November 2, 2016 2016-R-0274

UTILITY CYBERSECURITY

By: Mary Fitzpatrick, Legislative Analyst II

ISSUE

This report summarizes the Public Utility Regulatory Authority's (PURA) recent efforts on cybersecurity in the utility industry. For a glossary of cybersecurity terms, see OLR Report 2016-R-0267.

SUMMARY

In 2016, PURA established the Cybersecurity Oversight Program in which utility companies will voluntarily meet with PURA and the Division of Emergency Management and Homeland Security (DEMHS) to discuss company cybersecurity programs. Certain water, electric, and gas companies have indicated they will participate. Most telecommunications companies have declined to participate at this time.

PURA has designated certain topics for discussion at the annual meetings, including the company's cybersecurity program, its management's commitment to cybersecurity, and any results of recent third-party assessments. Participating companies must use an industry-accepted reporting standard.

To address concerns regarding disclosure of sensitive information, meetings will be private and the government agencies involved will retain no records.

In addition to PURA's program, a new position in the executive branch, the Chief Cyber Security Risk Officer, will be responsible for cybersecurity prevention and protection efforts across agencies and sectors.

What Happened in the Ukraine?

In December 2015, the Ukraine experienced the first confirmed hacking to disable a power grid.

Perpetrators of the attack accessed corporate networks to disable substations, reconfigure back-up power supplies, and replace substation firmware (i.e., essential software).

The attack caused power outages for several hours and left some control centers functional through manual operation only. Approximately 225,000 customers lost power.

PURA'S CYBERSECURITY OVERSIGHT PROGRAM

PURA established its Cybersecurity Oversight Program in its Connecticut Public Utilities Cybersecurity Action Plan in April 2016. Under the program, PURA will hold voluntary annual cybersecurity review meetings for each participating utility company to meet with PURA and DEMHS representatives and discuss its (1) cyber defense programs, (2) cyber threat experiences over the prior year, and (3) anticipated corrective measures.

Participating Companies

As part of the docket that led to the oversight program's creation, PURA held technical meetings with company representatives from the various utility sectors (water, telecommunications, gas, and electric). During these meetings, the representatives expressed concerns, voiced opinions on various federal standards and frameworks, and communicated their willingness to participate.

United Illuminating and Eversource representatives generally supported the idea of annual meetings and indicated that they would adopt a self-evaluation tool (Electric Sector – Cybersecurity Capability Maturity Model (ES-C2M2)) created by the federal Department of Energy (DOE). Representatives from the Aquarion Water Company and the Connecticut Water Company also indicated that they would participate in annual review meetings and supported using the same ES-C2M2 tool for reporting.

According to the action plan, most of the telecommunications companies were unwilling to participate due to their concerns that PURA would not be able to ensure the confidentiality of sensitive information. According to PURA, the companies also expressed concern that the oversight program would be a compulsory mandate, thus conflicting with federal policy preference for voluntary mechanisms. The companies recommended that PURA instead pursue a national framework.

Discussion Topics

According to PURA, the annual review meetings are meant to determine if a utility company is taking necessary steps to (1) defend against cyber-attacks, (2) detect and respond to attacks, and (3) restore affected capabilities or services after an attack. Meetings review the company's:

1. management's commitment to cybersecurity;
2. culture of cybersecurity;
3. cybersecurity program status, which includes an executive-level summary of the company's security posture, a description of new cybersecurity developments, and a cybersecurity risk register;

4. engagement with external cyber expertise;
5. third-party security assessments results; and
6. technical review of its cybersecurity program, which includes specific reporting standards, security controls, and industry best practices.

Reporting Standards

According to PURA, a company's report on its cybersecurity program should describe management processes, controls and safeguards, and successes and obstacles. PURA is requiring participating companies to use an industry-accepted reporting standard (e.g., ES-C2M2 or other similar federal standards), but is not requiring any specific standard.

Disclosure

According to PURA, to protect against disclosure of sensitive information, the meetings will be (1) held at the utility's office or other mutually agreed upon place and (2) private, with only PURA and DEMHS representatives unless otherwise agreed upon in advance. PURA and other government participants will not retain records in any format or take custody of confidential information and all participants will be bound by a non-disclosure agreement.

PURA also states that additional legislation to protect utility information is unnecessary, as such information is already protected under the federal Cybersecurity Act of 2015 and state law (CGS § 1-210(b)(19), –210(b)(20)).

CHIEF CYBER SECURITY RISK OFFICER

In October 2016, the governor announced the creation of a new position in the executive branch. According to the press release, the state Chief Cyber Security Risk Officer will be responsible for cybersecurity prevention and protection efforts across agencies and sectors. The position is housed within the Department of Administrative Services' Bureau of Enterprise Systems and Technology.

MF:bs